### 수집 모델 생성

새 수집 모델을 추가합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/logger-models

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="NGINX" \ -d logger\_factory\_name="dirwatch" \ -d 'rules=[{"name": "Web log", "log\_schema\_code": "web", "stream\_query": "rex field=line \"(?<src\_ip>\\S+) \\S+ \\S+ \\[(?<event\_time>\\S+ \\S+)\\] \\\"\\S+ \\S+ \\S+\\\" (?<status>\\d+) (?<sc\_bytes>\\d+) \\S+ \\\"(?<user\_agent>[^\\\"]+)\" | eval event\_time = date(event\_time, \"dd/MMM/yyyy:HH:mm:ss Z\"), src\_ip = ip(src\_ip), sc\_bytes = long(sc\_bytes)", "stream\_interval": 0}]' \ -X POST https://HOSTNAME/api/sonar/logger-models

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 수집 모델 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 수집 모델 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집 모델 설명 | 최대 2,000자 |
| logger\_factory\_name | O | 문자열 | 수집 유형 식별자 |  |
| parser\_code | X | 문자열 | 파서 식별자 |  |
| rules | X | 객체 배열 | 정규화 규칙 목록 | 하단 참조 |

rules 속성

* **guid** (문자열): 정규화 규칙 식별자. 미설정 시 무작위 식별자 부여.
* **name** (문자열): 정규화 규칙 이름
* **log\_schema\_code** (문자열): 로그 스키마 식별자
* **stream\_query** (문자열): 스트림 쿼리 문자열
* **stream\_interval** (32비트 정수): 스트림 쿼리 새로고침 주기

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

파서가 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "parser not found: nginx"}

수집 유형이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "logger factory not found: unknown"}

수집 모델 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated logger model name: NGINX"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}